

AusCERT2011

10th Annual AusCERT
Information Security Conference

15th - 20th May 2011

OVEREXPOSED



AusCERT

Security of Large Technical Systems

Marcus Sachs

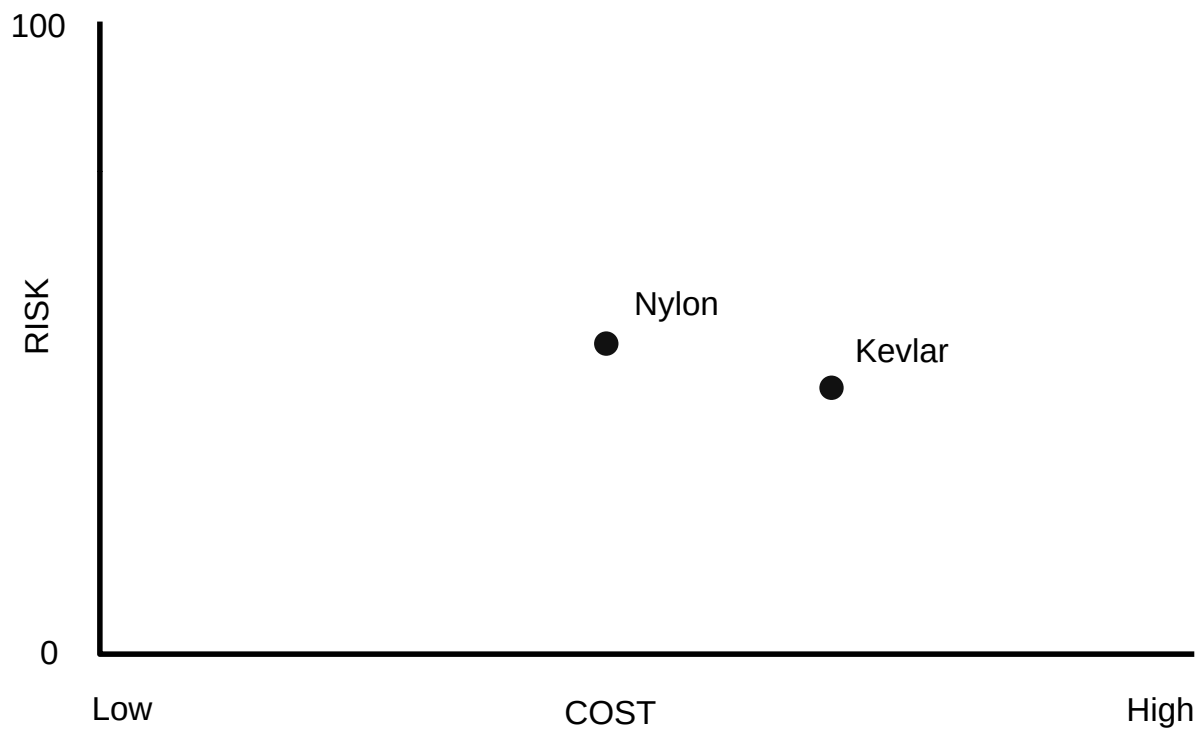
Vice President, National Security Policy

Verizon Communications

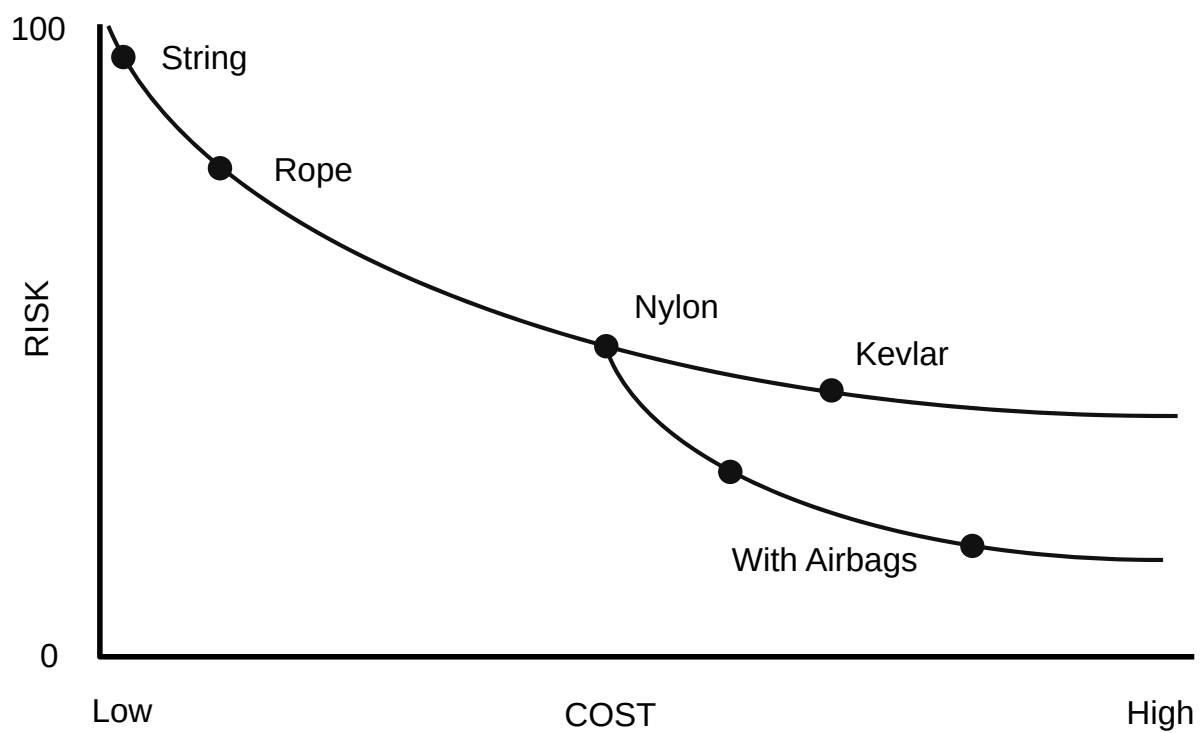
marcus.sachs@verizon.com

Before We Get Started....

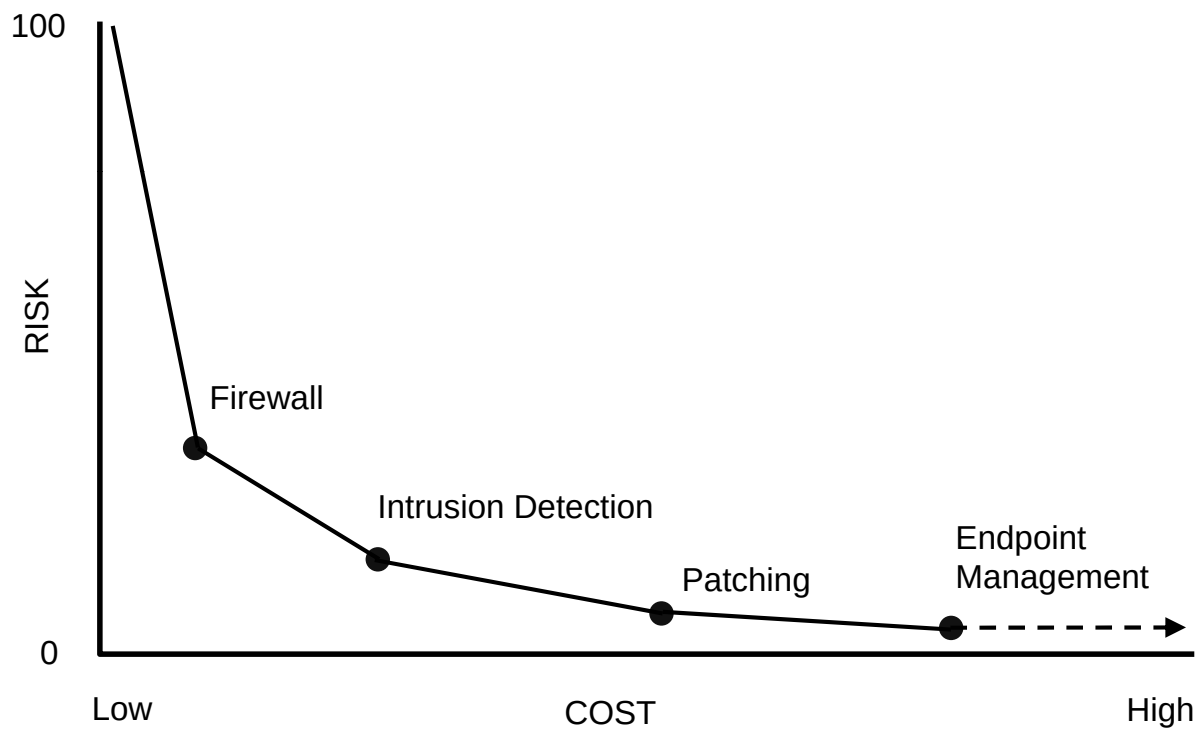
The Seatbelt Project



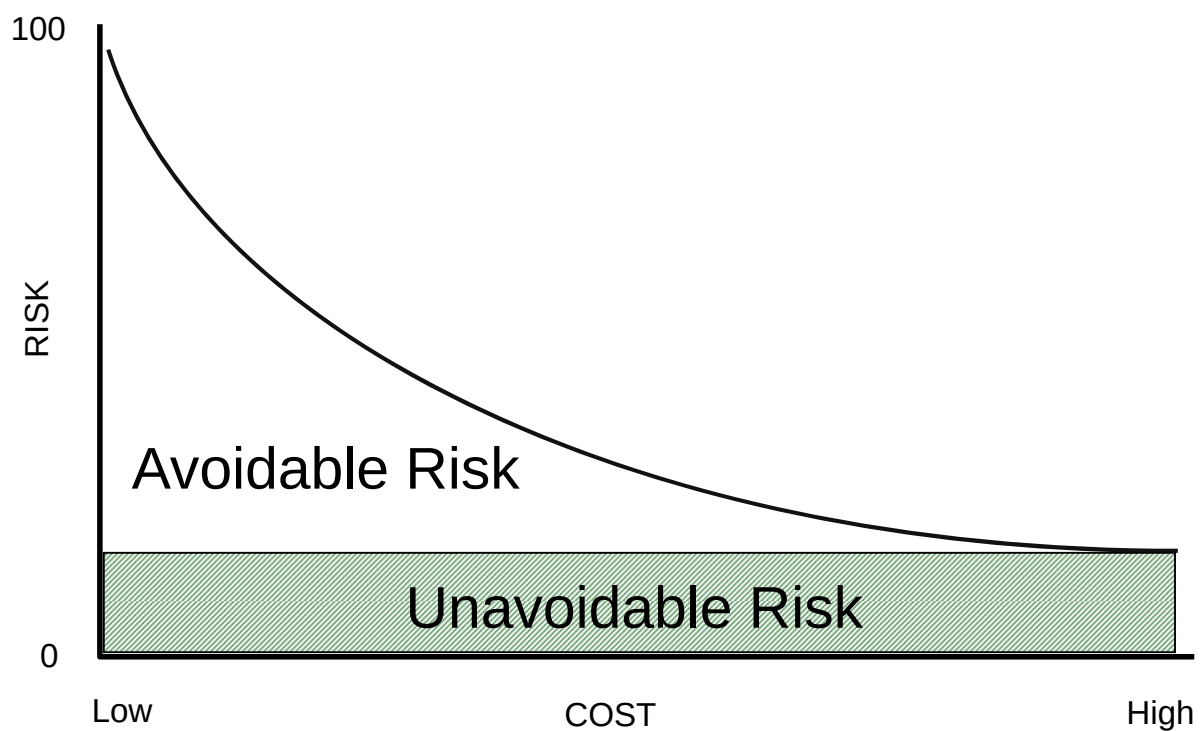
The Seatbelt Project



The Security Project



Managing Risk



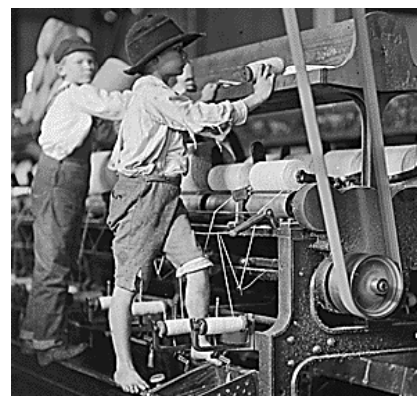
Introduction – The Industrial Age

- Development and growth of machinery and technology designed to simplify or replace manual tasks
- Early simple methods of mechanization and automation led to today's highly complex systems
- Required new techniques for control and management to prevent catastrophic failure or destruction
- Governments and legal systems reacted in various ways, not always positive

6

Industrial Age Technologies

- Late 1700s Textiles, iron making, and steam power
- 1793 Cotton gin
- 1807 Steamboat service
- 1812 Gas lighting in cities
- 1836 Telegraph
- 1825 Steam locomotive and railways
- 1858 Internal combustion engine
- 1866 Transatlantic cable
- 1876 Telephone
- 1879 Light bulb
- 1888 Electric motor
- 1892 Diesel engine
- 1903 Airplane
- 1913 Automotive assembly line



The Growth of Large Technical Systems

- The post-World War II era, especially the early years of the Cold War, were characterized by an explosion of Large Technical Systems (LTSs)
 - Term was coined by technical historian Thomas Hughes in his 1983 book "Networks of Power: Electrification in Western Society 1880 – 1930"
- LTSs brought together pieces invented during the Industrial Age
 - "Intelligent control" was needed to manage an LTS
 - Computers, both analog and digital, became the "brains" of an LTS

8

Examples of Large Technical Systems

- Nuclear missile early warning systems
- Air travel (traffic control, reservations, fly-by-wire aircraft)
- Energy grids (electric, gas, petroleum)
- Communications networks
- Banking and financial systems, including computerized stock trading
- Railroads, highways, shipping canals
- Space vehicles and support systems
- Nuclear power (fuel as well as the facility)

9

Large Technical *Networks* vs *Programs*

- Large Technical Systems can be divided into two subgroups:
 - Large Technical Networks (LTNs)
 - Transportation systems
 - Communication networks
 - Electric power grids
 - Large Technical Programs (LTPs)
 - Manhattan project
 - Space Shuttle program
 - Nuclear fusion reactor
- LTNs have closely-coupled components
- LTPs are pre-infrastructureal

10

Industrial Age vs Information Age LTSs

- Early LTSs were easy for an average person to understand
 - Mostly mechanical in their construction, with linkages, wheels, cams, rods, levers, switches, relays, and other devices
 - Simulated various physical parts of the human body (arms, legs, elbows, fingers, etc.) only on a much grander scale
- Older mechanical LTSs were linear, rational, and predictable
 - Internal feedback and control mechanisms that were also mechanical

11

Are We Building Frankenstein?

- Compare this to some modern examples: thermonuclear power plants, the Internet, air traffic control systems, electric power grids, and the global financial system
- Today's LTSs are no longer just large semi-predictable mechanical systems
 - They are non-linear, non-mechanical, non-rational systems that are typically controlled by one or many computerized "brains"
- They are systems that are increasingly based on *artificial intelligence* rather than just artificial muscles and bones

12

How Do You Govern Chaos?

- Today's LTSs might do unpredictable things
 - This is a known characteristic of chaotic systems
- In fact, we have likely moved to an era of Large Technical *Chaotic* Systems
- If true, it might help explain some of the difficulties organizations face with respect to understanding and mitigating external and internal threats that target today's LTSs
 - Organizations are like assembly line processes
 - Linear, rational, predictable
 - Very much like a 19th Century mechanical system

13

Linear vs Non-linear Management

- Governments and most business organizations are mechanical and rational
- Most are based on organizational theory adopted during the Great Depression
 - Developed in the era of mechanical LTSs
 - Lessons learned from the Ford Motor Corporation's operation and management of their automotive assembly lines greatly influenced the thinking of government and business leaders in the 1930s
 - Today's bureaucratic hierarchy reflects that thinking
- But today's society and certainly today's LTSs do not mirror the 1930s
 - Neither do the threats against our critical infrastructures, which have become just as complex in their organization as the attack and exploitation tools available to them

14

The Domains of Complexity in Power Systems

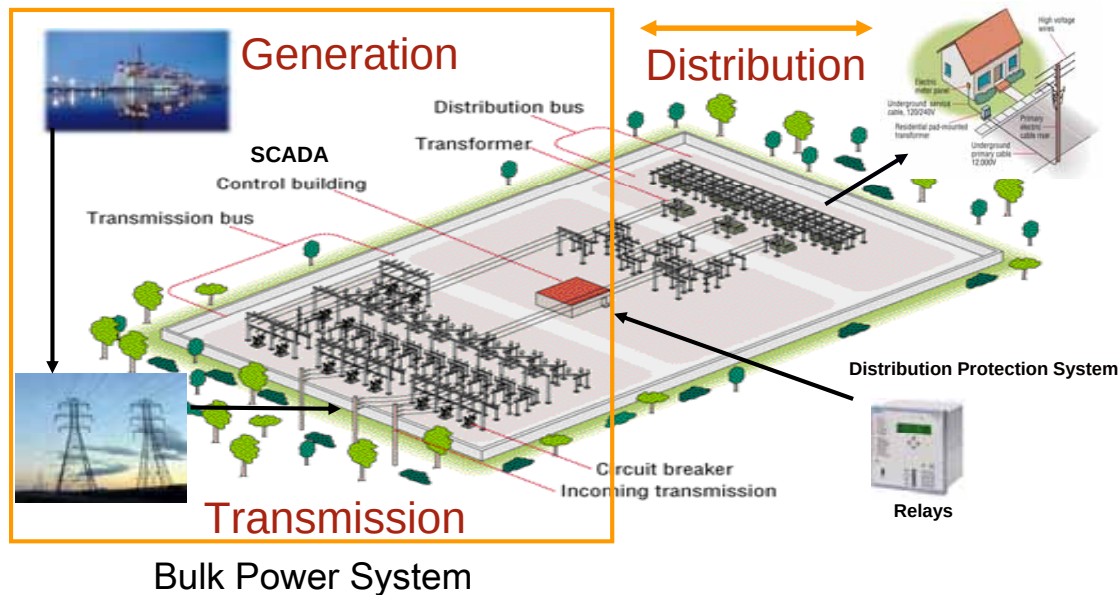
- Physical Power Components
- Telecommunications, IT and Control Systems
- Operational and Organizational
- Standards and Regulatory



15

Power System Components

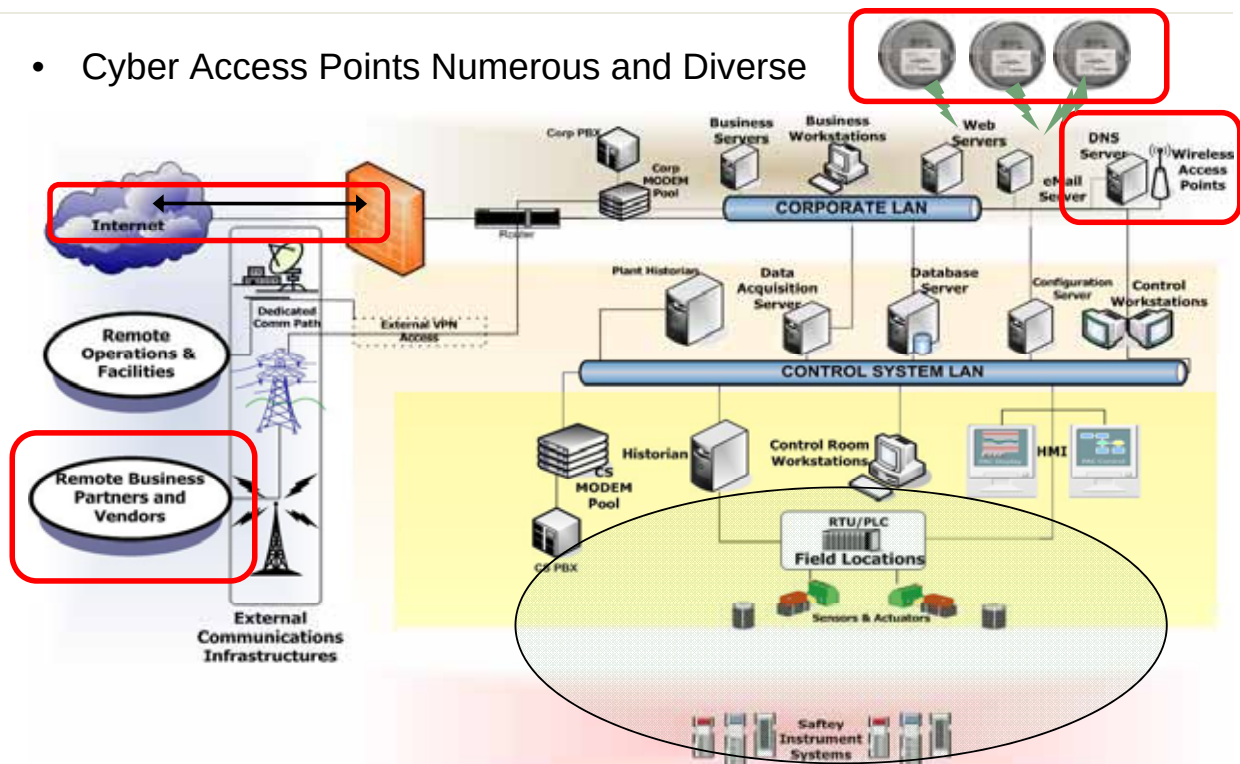
- Physical Access Points Numerous and Diverse



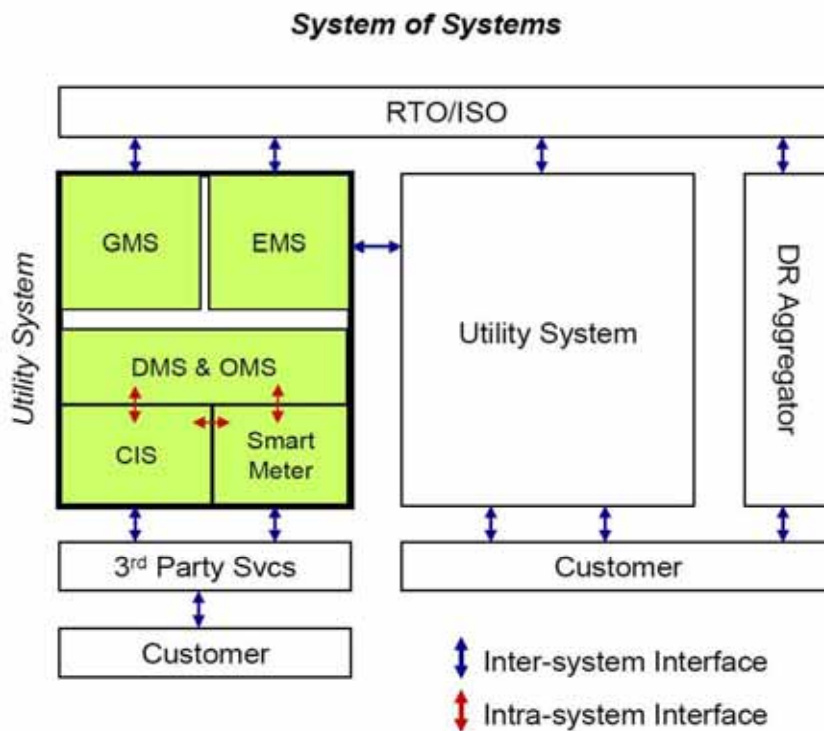
16

Communication System Components

- Cyber Access Points Numerous and Diverse



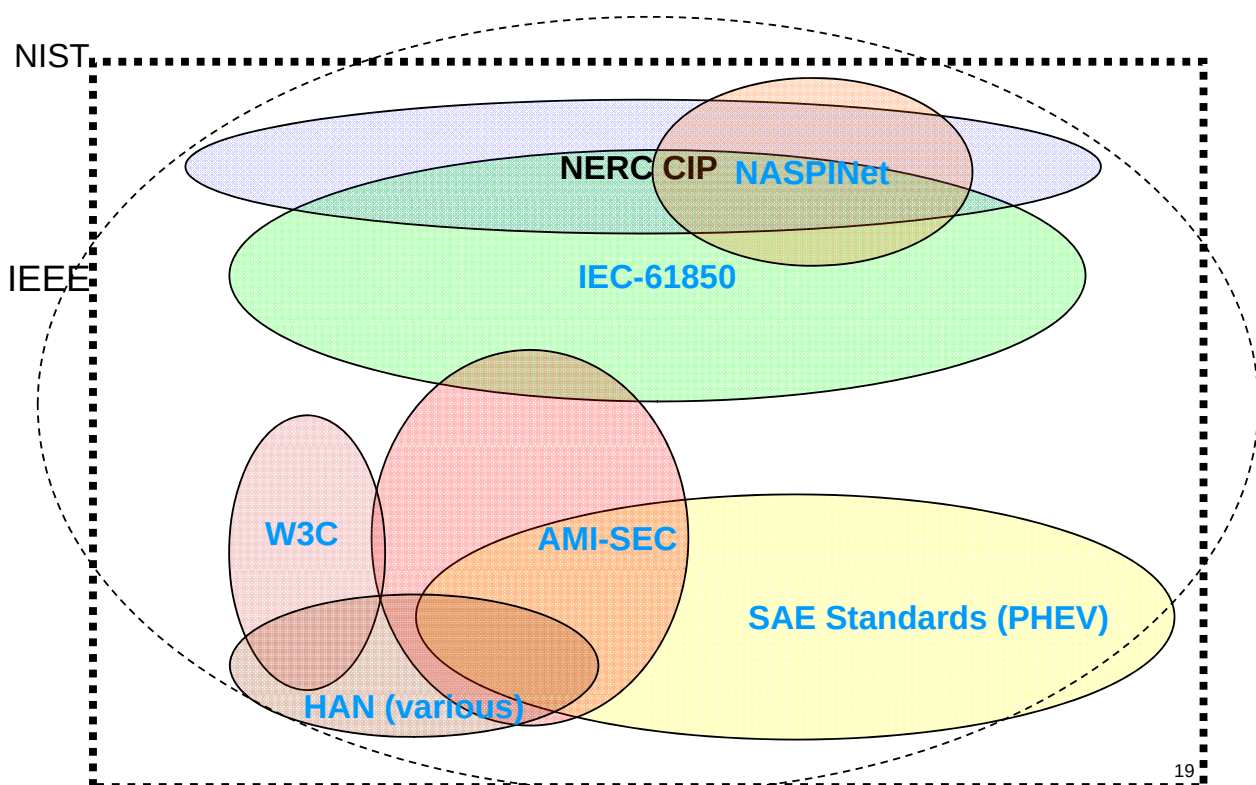
Operational Components



ISO: Independent System Operator
RTO: Regional Transmission Org.
GMS: Generation Mgmt. System
EMS: Energy Mgmt. System
DMS: Distribution Mgmt. System
OMS: Outage Mgmt. System
CIS: Customer Information System

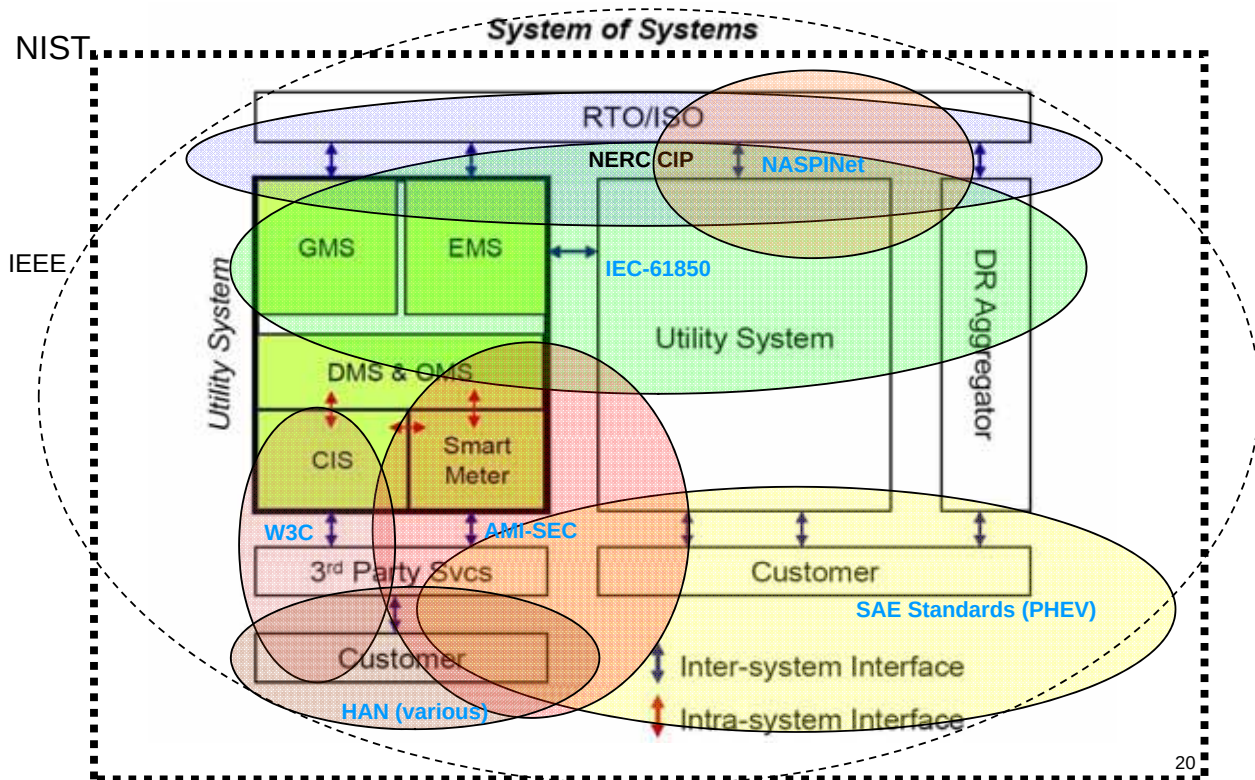
18

Standards and Regulatory Components



19

Complexity - Overlay Everything



Complexity leads to

- System collapse into smaller simpler collections.
 - Micro-grids and islanding (think about nuclear power plants)
 - Walled gardens
- OR
- Unpredictable behaviors emerge
 - New integration (“just in time” delivery)
 - System failure (cascading service outage)
 - Government failure or regime change (Egypt, Libya, Yemen, etc.)

When Complexity Meets Humans

- Large industrial-age mechanical systems were easy for people to understand and control
 - Steam locomotive (or an entire railroad)
 - Ford Model T (or a Ford assembly plant)
- Today we have highly complex and interdependent infrastructures, platforms, and systems
 - Electric grids
 - Fly-by-wire aircraft (and even automobiles)
- Computers and computer systems are needed to manage what is beyond the capacity of a person
- But what happens when the computer systems fail?

22

Air France Flight 447, May 2009

- Airbus A330-200 lost communication about 3-1/2 hours after take-off from Brazil
 - Most likely cause was loss of control as the aircraft passed through thunderstorms over the Atlantic
 - Black boxes and other computer systems were found two years after the event – no conclusions yet
- A330 is a “fly by wire” airframe that uses three primary and two secondary computers
- Pitot probe failure due to icing is most likely cause



Washington, D.C. MetroRail Crash, June 2009

- MetroRail crash avoidance system failed to stop a south-bound train
- Investigations revealed that the system had failed more than once prior to the crash
 - Of 668 incidents that caused delays in 2008, track circuits accounted for 337
- At the time of the crash, the train speeds were set by an on-board computer
 - The train operator attempted to stop the train with the emergency brakes, but did not override the computer



Sayano-Shushenskaya Dam, August 2009

- Before the accident, was the largest hydroelectric plant in Russia, sixth largest in the world
- The 920-ton rotor of turbine #2, known for several years to have mechanical problems, lifted out of its seat
- Computers failed to shut down the turbine
- Water flow had to be manually turned off



NYSE “Flash Crash”, May 2010

- Fortunately no loss of life
- DOW dropped more than 600 points in five minutes, regained the 600 points in 20 minutes
- Triggered by a large mutual fund firm selling an unusually large number of E-Mini S&P 500 contracts
- “Crash” resulted from actions taken by the computerized trading system



Stuxnet vs the Iranians, 2010

- Stuxnet is malware that appears to have been written to target Iranian nuclear centrifuges
- Makes practical what previously had been theoretical (physical destruction via software manipulation)
- No country, group, or organization has yet claimed ownership



Other Examples

- 1986 and 2002 Space Shuttle mishaps
- 2003 Canada/US electric power blackout
- 2008 Spanair flight 5022 crash on takeoff
- 2010 explosion and sinking of the Deep Water Horizon oil rig in the Gulf of Mexico
- 2011 Fukushima Daiichi nuclear power plant in Japan



When Complex Systems Fail

- All of us -- engineers, policymakers, the media and the public -- have a role to play in ensuring that proper practices are in place to minimize the risks inherent with critical complex systems
- Regardless of whether the complex system in question is an oil rig in deep water, a nuclear power plant, a spacecraft or even a long-haul jet, engineers and others involved in design, regulatory or maintenance processes have a moral imperative to fully examine not only the development and operation of these complex systems, but also their "fault-tolerance"

Conclusion: Is Failure an Option?

- A better question might be, “is failure normal?”
- If we agree that Large Technical *Complex* Systems can, and will, fail for any of a large number of reasons – then how do we manage that risk?
 - Can we prevent failure?
 - Or should we try to manage failure?
- Remember the “security project” we talked about earlier
 - Perfect security (or safety) is rarely achievable
 - Best to understand your risk tolerance level, then manage the risk to that level

30

Be Mindful of Emergent Behaviors

